21(b), for example.

That phrase, in referring to the "records" which were stored in claim 21(a), clearly refers to a **group of records selected from** the "records" of claim 21(a). There is no ambiguity or lack of clarity.

A similar comment applies to the other rejected claims.

Point 2

Applicant points to claim 2 in US patent 5,288,949, which states:

> 2. A carrier for integrated circuits, comprising:
>
> a) no more than two layers of conductors;
>
> b) interconnections among the conductors such that
>
> > i) **some** conductors can be used as signal conductors; and
> >
> > ii) other conductors can be used as power conductors which shield the signal conductors from each other.

In view of the use of the word "some" in this patent, which was clearly approved by the PTO, Applicant requests a citation of a court decision in support of the rejection.

RESPONSE TO 103 - REJECTIONS

Kawan Reference not Available

The publication date of the Kawan reference is May 23, 2002. However, Applicant's filing date is August 31, 2000, which precedes Kawan's data by almost two years.

Applicant points out that the filing date of Kawan, as opposed to the publication date, is not relevant, because Kawan is not a patent.

Thus, the Kawan reference is not available for use against this application.

Claim 21

Point 1 - All Claim Elements not Found in References, Even if Combined

Overview of Point 1

Kawan discusses using a PDA to communicate with an ATM. Menezes discusses generalized aspects of encryption.

At least four claim recitations are absent from Kawan. They are listed below, after this Overview. The addition of Menezes to Kawan does not cure this absence of claim recitations in Kawan.

Two of the missing recitations will be discussed in this Overview.

ONE MISSING RECITATION

One missing recitation is this. Claim 21 recites

-- generating a key K1 in a portable computer,

-- encrypting K1,

-- transmitting K1(encrypted) to an external terminal, and

-- receiving an "encrypted response."

Significantly, the "encrypted response" is in "response" to the receipt of K1(encrypted). The "encrypted response" is not merely an encrypted message. It is a "response."

No such "encrypted response" is found in the references, even if combined.

-- No encrypted message is received by Kawan's PDA.

-- Nor is any such message received as a "response" to an encrypted key.

Menezes cannot be used to supply this missing recitation, because it is simply not found in Menezes.

SECOND MISSING RECITATION

Another missing recitation is this. Claim 21 recites

-- receiving an encrypted message (the "encrypted response" above) in a portable computer, and

-- decrypting it using a certain key, K1, which was previously generated by the portable computer.

But no such message is received by Kawan's PDA. And no decryption of the (absent) message by K1, previously generated in the PDA, is shown in Kawan.

There is an encrypted message present in Kawan: Kawan's PDA sends an encrypted message **TO** an ATM, which message contains a PIN and biometric data. But that does not show claim 21, which recites **receiving** an encrypted message in a portable computer.

And it makes no sense for the ATM of Kawan to send the claimed "encrypted response" to Kawan's PDA. One reason is that the encrypted message sent **from** Kawan's PDA **to** the ATM contains

(1) a PIN and

(2) biometric data, such as a scanned fingerprint.

That makes sense: the ATM wants to identify the owner of the PDA.

But it makes **no sense** for the ATM to send such data to Kawan's PDA.

-- ATMs do not have PINs,

-- ATMs do not have fingerprints, and

-- ATMs do not verify themselves to customers.

CONCLUSION

Therefore, several claimed processes are not present in Kawan, and two have been discussed. Menezes does not show those missing processes. Thus, even if the references are combined, claim 21 is not shown.

End Overview

Resumption of Point 1

Several elements of claim 21 are not found in the Kawan and Menezes references, even if combined, as will now be explained.

Claim 21 recites using a portable computer to

1) generate an encryption key K1,

2) encrypt K1,

3) transmit K1(encrypted) to an external terminal,

4) receive an "encrypted response" from the external terminal, and

5) de-crypt that response **using the same key K1**.

Kawan does not Generate Keys in PDA Nor Perform Encryption in PDA

Claim 21 states that, in the portable computer, key K1 is derived from a seed, and then encrypted.

Kawan discusses use of a PDA, Personal Digital Assistant, to communicate with an ATM, Automated Teller Machine. But Kawan does not discuss generation of keys within the PDA, so the claimed derivation of K1 from a seed is not present in Kawan.

Nor does Kawan discuss performing encryption in his PDA. The closest discussion is found in paragraph 31, where he discusses using an encrypted PIN (Personal Identification Number) and encrypted biometric information (eg, a fingerprint). However, he does not discuss **performing** encryption on those two elements **within the PDA**.

And that lack of encryption within the PDA makes sense. The PIN and the biometric information will not change. They are constant. It would waste processing power to repeatedly encrypt those two elements every time a transaction takes place.

Further, why would plain text of the PIN/biometrics be stored within the PDA, for encryption for each transaction ? If the PDA were lost, the finder would obtain access to them.

Thus, it is reasonable to assume that Kawan stores those two elements (PIN/biometrics) **in encrypted form**.

Consequently, no encryption occurs in Kawan. And Kawan produces no keys in his PDA. Two claim elements are missing from Kawan: (1) generating K1 from a seed, and (2) encrypting K1. MPEP § 2143.03 states:

> To establish prima facie obviousness . . . **all the claim limitations** must be taught or suggested by the prior art.

Even if Menezes shows these recitations in the abstract sense, adding Menezes to Kawan does not produce claim 21. Claim 21 states that the two claim elements are performed within the "portable computer." As explained herein, adding the two claim elements to Kawan's PDA makes no sense. This shows (1) lack of motivation to do it and (2) lack of the required expectation of success, as explained below.

Further, even if Kawan does encrypt the PIN and biometric data, that does not show claim 21, which recites encryption of a **key**.

Direction of Message in Kawan is OPPOSITE to that Claimed

As stated above, the only encrypted elements of Kawan are (1) the PIN and (2) the biometric information.

But claim 21 states that an encrypted response is received by the "portable computer" and de-crypted therein. That is not shown in Kawan's PDA (which is the only element in Kawan which could correspond to the claimed portable computer).

Kawan transmits his encrypted matter **FROM** his PDA **TO** the ATM, to verify the authenticity of the PDA. That transmission is in the **opposite direction** to the transmission of the "response" in claim

21.

And, in Kawan, there is no reason to transmit the encrypted matter (PIN/biometrics) in the direction claimed (ie, from the ATM to the portable computer). One reason is that no encrypted matter exists in the ATM, which could be transmitted to the PDA.

That is, the ATM has no PIN or biometric data which could be sent to Kawan's PDA. Nor would that make any sense: ATMs do not have PINS, nor do they have fingerprints.

Therefore, no transmission of an encrypted response in the claimed direction is found in Kawan. And such transmission would be impossible: no data usable in such a transmission is present in Kawan.

Claimed "Response" is Absent from Kawan

Claim 21 recites an "encrypted response." The "encrypted response" is produced in response to the transmission of K1(encrypted).

No corresponding "response" is found in Kawan.

Claimed De-Cryption of "Message" is Absent from Kawan

Since, as just explained, no encrypted message/response is received by Kawan's PDA, no de-cryption of that (absent) message can occur. Thus, the de-cryption of claim 21(c) is necessarily absent, as is using key K1 to perform the (absent) de-cryption.

Interim Conclusion

Therefore,

-- Kawan's PDA performs no key generation.

Thus, the claimed generation of K1 from a seed is absent.

-- No encryption is performed by Kawan's PDA.

Thus, the claimed generation of K1(encrypted) is absent.

-- Kawan may transmit encrypted matter **from** his PDA **to** the ATM, but that is in the **wrong direction**, compared to the claim language.

Thus, the claimed receipt of the encrypted message by the portable computer is absent from Kawan.

-- Since Kawan's PDA does not receive an encrypted message, his PDA cannot de-crypt any such message.

Thus, the claim language "receiving an encrypted response from the external terminal, and de-crypting the encrypted response using the plain text of K1" as in claim 21(c) is absent from Kawan.

-- Since Kawan's PDA does not generate any key K1, it cannot use that same key K1 to decrypt the (absent) message received from the ATM.

> Thus, use of **a previously generated** K1 to de-crypt the claimed message is absent from Kawan.

-- Claim 21 recites an "encrypted response," which is received as a "response" to transmission of K1(encrypted). No such "response" is found in Kawan.

> Thus, the "encrypted response" of claim 21(c) is absent from Kawan.

These six elements of claim 21 are absent from Kawan.

The addition of Menezes does not rectify these absences, since Menezes does not show these elements either. Menezes just discusses generalized aspects of encryption.

Stating this another way, the only possible relevance of Menezes lies where Kawan discusses encrypted data. But even if Menezes is added to Kawan in that aspect, claim 21 is still not attained, because the missing elements described above are not supplied.

Consequently, these six claim elements are not found in the references, even if combined. MPEP § 2143.03, cited above, precludes the rejection.

Point 2 - Request for Identification

Applicant, under 37 CFR §§ 1.104(c)(2) and 35 U.S.C. § 132, requests that the following elements of claim 21 be identified in the references:

1) the "seed,"

2) the key K1,

3) the "encrypted response,"

4) the "encrypted response" received by a "portable computer," and

5) de-crypting the "encrypted response" using K1.

Point 3 - PTO is Modifying Kawan

The PTO is modifying Kawan. MPEP § 2143.01 prohibits this:

> THE PROPOSED MODIFICATION CANNOT RENDER THE PRIOR ART UNSATISFACTORY FOR ITS INTENDED PURPOSE.
>
> . . .
>
> THE PROPOSED MODIFICATION CANNOT CHANGE THE PRINCIPLE OF OPERATION OF A REFERENCE.
>
> . . .
>
> If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious.

That is, the PTO is

-- Adding key-generation (K1) to Kawan's PDA, where Kawan has none.

-- Adding encryption of the generated key K1 to Kawan's PDA, where Kawan has none.

-- Adding transmission of an encrypted message **from** Kawan's ATM **to** the PDA. But that message appears to serve no purpose, and no purpose has been stated.

-- Adding de-cryption of that (non-existent) message.

-- Using a non-existent key, K1, to de-crypt the non-existent message.

The MPEP section cited above precludes the rejection.

Point 4 - No Expectation of Success Shown

MPEP § 706.02(j) states:

> Contents of a 35 U.S.C. 103 Rejection
>
> . . .
>
> To establish a prima facie case of obviousness, three basic criteria must be met.
> . . .
> Second, there must be a reasonable expectation ofsuccess.
> . . .
> the reasonable expectation of success must

> . . . be found in the prior art and not based on applicant's disclosure.

As explained above, several claim elements are missing from Kawan. Even if those elements are supplied by Menezes, which is not possible, the PTO must still show an expectation of success. That has not been done. Some examples of lack of expectation of success are illustrated by the following questions.

> -- What is the purpose of the claimed "encrypted response" of claim 21 (which is de-crypted by K1) if added to Kawan ?
>
> -- Why would the PDA encrypt and deliver key K1 to Kawan's ATM, when the ATM already has an encryption key, which is used to de-crypt the PIN and the biometrics ?
>
> -- The only encrypted matter in Kawan, as explained above, contains (1) the PIN and (2) the biometric data. Why would that encrypted matter be transmitted **to** Kawan's PDA, as a "response" to receipt by an encrypted key K1, received by the ATM ?
>
> -- Why would Kawan transmit the "encrypted response" of claim 21, which would travel **from** Kawan's ATM **to** his PDA ?

Until these, and other, questions have been answered, Applicant submits that no "expectation of success" has been shown, as required by the MPEP.

Point 5 - No Teaching for Combining References Given

No valid teaching for combining the references has been given.

The rationale given for combining the references is given in the Office Action, page 4, second full paragraph. That rationale asserts that three motivations lead to a combination of the references, namely,

1) attainment of a true random sequence for a key,

2) "to limit available cipher text for cryptanalytic attacks," and

3) attainment of protection of the session key.

However, several problems exist in these motivations.

PROBLEM 1

As Menezes states, attainment of a truly random sequence is "a difficult task." (Page 171, section 5.2.) And none of the approaches shown in Menezes, page 172, lead to truly random bit sequences.

Therefore, the assertion that the combination of references leads to a "truly random sequence" is highly suspect. As a minimum, it is a conclusion unsupported by evidence. Evidence is required.

PROBLEM 2

As a continuation of Problem 1, the undersigned attorney points out that, in effect, the PTO is asserting that the combination of references allows an ordinary PDA to become a perfect random number generator. This would be an achievement of Nobel-Prize-rank. Applicant offers to submit an affidavit on this point, if the Examiner so requests.

That conclusion is suspect on its face, and demands further support.

PROBLEM 3

Even if a "truly random sequence" is sought, the **combination** of references is not needed to attain it. That is, if the PTO is correct, and Menezes provides "truly random sequences," then Menezes, **by himself**, provides those sequences. There is no reason to add Kawan.

That is, the goal is attained by **ONE** reference alone. The other reference is not needed.

PROBLEM 4

The second motivation is "to limit available cipher text for cryptanalytic attacks." Applicant submits that this motivation is self-defeating.

The Office Action actually **adds** cipher text to Kawan (eg, the "encrypted response" of claim 21(c)). That does not "limit" available cipher text, but **increases** available cipher text.

PROBLEM 5

The fifth motivation is to protect the session key. However, this is a conclusion lacking support. It has not been shown how the combination of references actually provides any protection.

Restated, the Office Action merely asserts that the combined references show claim 21, but without detailed explanation. An explanation is required as to how the motivation of protecting the session key leads to claim 21.

That is, you can combine references and protect a session key, without attaining claim 21. The Office Action must show how the combination of references not only protects a session key, but also attains claim 21.

In addition, claim 21 does not recite protecting a session key. Nor has the Office Action shown how the combined references protect the session key.

Point 6 - References Teach Against Claim 21

Sub-Point 6A

Claim 21(a) states that the "records" are stored in "user-accessible memory." Claim 21(b) states that the "seed" for key K1 is generated from the "records."

Thus, any user of the claimed "portable computer" has access to the "records." That is contrary to Menezes' teachings.

Menezes, in section 5.2, states that "A random bit generator requires a . . . source of randomness." Under claim 21, the "source of randomness" would be the claimed "records." Thus, under claim 21, the "source of randomness" would be "user-accessible."

But Menezes' section 5.2 also states, "The generator must not be subject to observation." That is contrary to storing the "records" in "user-accessible memory," as claimed.

Thus, Menezes teaches against claim 21.

Also, Menezes' section 5.2(ii) lists some events which may be similar to those in the "records" of claim 21. But Menezes states that an "adversary" should be prevented from "observing" those events. (Menezes, section 5.2(ii), fourth sentence.) Again, that is opposite to claim 21, which states that those events are stored in "user-accessible memory."

Menezes teaches against claim 21.

Sub-Point 6B

At least two possibilities exist in Menezes. One is that Menezes

1) stores the events in memory then

2) later reads the stored events, and

3) then applies the read/stored events as inputs to an algorithm, to produce a key.

Another possibility is that Menezes eliminates steps (1) and (2), and applies the events directly to the algorithm, to produce a key.

If the latter possibility occurs, then the recited storage of claim 21(a) is not found in Menezes. Claim 21(a) is not found in the references, even if combined.

Point 7 - "Records" in "User-Accessible Memory" used for "Seed" Not Shown in References

Claim 21 recites a "portable computer," and

> a) storing records of events experienced by the computer in user-accessible memory within the computer.

Claim 21 also recites using some of the "records" as a "seed" for producing a cryptographic key K1.

That has not been shown in the applied references.

Applicant thus requests that following be identified in the applied references:

-- The "records,"

-- The "user-accessible memory," and

-- The "seed."

Conclusion as to Claim 21

Even if the references are combined, several claim elements are missing.

No valid teaching has been given for combining the references.

Menezes teaches against the concept of deriving a "seed" from data stored in "user-accessible memory."

No expectation of success has been shown. For example, no explanation has been given of what the claimed "encrypted response" would do, if added to Kawan.

Remaining Claims

The preceding discussion applies to the remaining claims. Specifically, the "Interim Conclusion" given above is here repeated, which shows that several elements are absent from the references, even if combined.

Interim Conclusion (Repeated)

-- Kawan's PDA performs no key generation.

Thus, the claimed generation of K1 from a seed is absent.

-- No encryption is performed by Kawan's PDA.

> Thus, the claimed generation of K1(encrypted) is absent.

-- Kawan may transmit encrypted matter **from** his PDA **to** the ATM, but that is in the **wrong direction**, compared to the claim language.

> Thus, the claimed receipt of the encrypted message by the portable computer is absent from Kawan.

-- Since Kawan's PDA does not receive an encrypted message, his PDA cannot de-crypt any such message.

> Thus, the claim language "receiving an encrypted response from the external terminal, and de-crypting the encrypted response using the plain text of K1" as in claim 21(c) is absent from Kawan.

-- Since Kawan's PDA does not generate any key K1, it cannot use that same key K1 to de-crypt the (absent) message received from the ATM.

> Thus, use of **a previously generated** K1 to de-crypt the claimed message is absent from Kawan.

-- Claim 21 recites an "encrypted response,"

> which is received as a "response" to transmission of K1(encrypted). No such "response" is found in Kawan.
>
> > Thus, the "encrypted response" of claim 21(c) is absent from Kawan.

Menezes cannot be used to supply the missing claim elements, because they are not found in Menezes.

Each of the remaining claim contains one or more of the recitations just enumerated. As just explained, those recitations are not found in the references, even if combined. MPEP § 2143.03 states:

> To establish prima facie obviousness . . . **all the claim limitations** must be taught or suggested by the prior art.

The rejection does not comply with this MPEP section.

Additional Point 1

The Office Action , pages 4 and 5, only asserts that subject matter of claims 22 - 32, 34, and 38 is found in the two references. That is insufficient. MPEP § 706.02(j) states:

> Contents of a 35 U.S.C. 103 Rejection
>
> . . .
> After indicating that the rejection is under 35 U.S.C. 103, the examiner should set forth in the Office action:

> (A) the relevant teachings of the prior art relied upon, preferably with reference to the relevant column or page number(s) and line number(s) where appropriate,
>
> (B) the difference or differences in the claim over the applied reference(s),
>
> (C) the proposed modification of the applied reference(s) necessary to arrive at the claimed subject matter, and
>
> (D) an explanation why one of ordinary skill in the art at the time the invention was made would have been motivated to make the proposed modification.
>
> To establish a prima facie case of obviousness, three basic criteria must be met.
>
> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings.
>
> Second, there must be a reasonable expectation of success.
>
> Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.
>
> The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure.

The mere assertion that claim elements are found in the references is insufficient to support a rejection under section 103.

Additional Point 2

Claims 35 - 37 are dependent claims, and contain the phrase "wherein the portable computer requires entry of a Personal Identification Number, PIN, prior to encryption," or similar.

As explained above, Kawan does not perform encryption. Thus, the requirement of a PIN, as a prerequisite for the (non-existent) encryption is not found.

Further, the PIN is already stored in Kawan's device.

Additional Point 3

The references are contradictory, regarding a "session key." Menezes, top of page 494, states that a session key is used for a single transaction.

Kawan, paragraph 31, states that his encrypted PIN and biometric data can be used for a single transaction, or multiple transactions.

Contradictory references cannot be combined.

CONCLUSION

Applicant requests that the rejections to the claims be reconsidered and withdrawn.

Applicant expresses thanks to the Examiner for the careful consideration given to this case.

Respectfully submitted,

Gregory A. Welte
Reg. No. 30,434

NCR Corporation
1700 South Patterson Blvd.
WHQ - 4
Dayton, OH 45479
July 18, 2005
(937) 445 - 4956